ISSN: 0067-2904

A Framework of APT Detection Based on Packets Analysis and Host Destination

Khalid Abdulrazzaq Abdulnabi Alminshid[1*], Mohd Nizam Omar[2]
[1]General Directorate of Education in Thi-Qar province, Ministry of Education, Iraq, Thi-Qar, Iraq
[2]School of Computing, InterNetWorks Research Laboratory, Universiti Utara Malaysia, Kedah, Malaysia

Received: 3/6/ 2019 Accepted: 18/ 8/2019

Abstract

So far, APT (Advanced Persistent Threats) is a constant concern for information security. Despite that, many approaches have been used in order to detect APT attacks, such as change controlling, sandboxing and network traffic analysis. However, success of 100% couldn't be achieved. Current studies have illustrated that APTs adopt many complex techniques to evade all detection types. This paper describes and analyzes APT problems by analyzing the most common techniques, tools and pathways used by attackers. In addition, it highlights the weaknesses and strengths of the existing security solutions that have been used since the threat was identified in 2006 until 2019. Furthermore, this research proposes a new framework that can be used to repel this threat based on APT activity with network traffic through packets analysis and host destination.

Keywords: detection, APT, Advanced Persistent Threats, traffic, intrusion.

إطار عمل الكشف عن التهديدات المستمرة المتقدمة استنادًا إلى تحليل الحزم ووجهة المضيف

خالد عبدالرزاق عبدالنبي المنشد[1]*، محمد نظام عمر[2]
[1]المديرية العامة للتربية في محافظة ذي قار, وزارة التربية, ذي قار, العراق
[2] كلية الحاسبات، مختبر أبحاث الإنترنت، جامعة أوتارا ماليزيا، قدح، ماليزيا

الخلاصة

حتى الآن ، تعتبر APT (التهديدات المستمرة المتقدمة) مصدر قلق دائم لأمن المعلومات. فعلى الرغم من وجود العديد من الطرق المستخدمة للكشف عن هجوم APT مثل تغيير التحكم ، وضع الحماية ، وتحليل حركة مرور الشبكة، إلا أنها ليست ناجحة 100٪. توضح الدراسات الحالية أن APTs تعتمد العديد من التقنيات المعقدة للتهرب من جميع أنواع الاكتشاف. تصف هذه الورقة البحثية وتحلل مشكلة APT من خلال تحليل التقنيات والأدوات والمسارات الأكثر شيوعًا التي يستخدمها المهاجمون. بالإضافة إلى ذلك ، فإنه تسلط الضوء على نقاط القوة والضعف في الحلول الأمنية الحالية التي تم استخدامها منذ أن تم تحديد التهديد في عام 2006 ، حتى عام 2019. علاوة على ذلك ، البحث يقترح اطارا جديدا يمكن ان يستخدم لصد هذا التهديد بالاعتماد على فعالية APT مع حركة مرور الشبكة , من خلال تحليل الحزم والوجهة المضيفة

Introduction

According to the latest reports released by Kaspersky and McAfee, Advanced Persistent Threats (APT) is one of the most serious threats facing information security [1, 2]. Several months or even years usually pass before detecting this type of threat samples [3]. APT is used by the most sophisticated criminals on the Internet, where this type requires high experience and patience to stealthily access to the data of public and private companies. APT's targets are usually one of the

*Email: khalid_uum@yahoo.com

public or private institutions such as health care companies, financial institutions, universities and government agencies.

The APT term represents three words that are Advanced, Persistent and, Threat. Advanced means that hackers who use APT have high skills, using the latest methods of infiltration and intrusion inside the company's system. Persistent represents a constant attack and usually implemented through a "low and slow" approach that depends on a period of continuous attack that may exceed months or years. Threat refers to the risk or danger from this type of intrusion [4].

Many techniques have been used to detect APT attacks such as change controlling, sandboxing and, network traffic analysis. However, all these techniques are classified into two categories [5]. First, signature-based techniques, which are unique features already stored in the antivirus. Second, behavior-based techniques, which are based on behavior analysis of malware during attack. Typically, APT groups use zero-day malwares which are not present in the antivirus database. Therefore, the unknown APT threat can easily evade detection [6-8]. On the other hand, behavior-based techniques have three limitations: high false alarm rate, complexity [9] and inability to detect a lot of polymorphic threats [10]. APT cannot be identified effectively with traditional detection technologies.

Given these limitations, the researchers began looking for a new technique that can detect APT attacks. Researchers found two weaknesses that could be used in this detection process. First, all APT threats share the steps taken during the attack, showing certain phases of the attack before reaching the ultimate goal [11]. Second, the data theft cannot be completely invisible; the theft of data needs outbound traffic. It is a successful way to discover APT attacks [12]. Therefore, this article discusses the problem of APT attacks and suggests a proposed method that can be effective in the face of this threat.

This paper is organized into the following structure: The current section contains the introduction and background of the research. Section 2 reviews, explores, and discusses the literature to establish the basis of the proposed framework. Section 3 illustrates the conceptual framework. Section 4 reviews the conclusion and future work.

Literature Review

This section discusses the previous works related to the subject of this research. The first part presents the history and details of the APT attacks from the perspective of the previous studies. The second part discusses how the previous studies analyzed the APT attack process and its life cycle. The third part shows how previous studies classified the APTs types and groups. The last part discusses and analyzes the methods and approaches that have been used to detect the APT attack. Furthermore, it discusses the advantages and disadvantages of each method.

Advanced persistent threats (APTs)

APTs are electronic attacks targeting a specific destination, usually a government or private institution. Typically, the goal of these cyber-attacks is often to steal valuable information that exists in the database of these institutions [13]. APTs attack is a major problem facing the information security and global networks [14]. APT attacks can be bundled with shareware or other download software. It is not difficult for many types of the APTs to pass the firewall of the system. They use advanced evasion techniques to hide their malicious behaviour and evade all traditional detection methods [15]. APTs are more sophisticated than traditional attacks such as viruses, trojans, malware, worms and, backdoors. Table-1 shows the comparison between the APT attacks and traditional attacks.

Table 1-Traditional attacks and APT attacks: comparison *Source:[16]*

Attacks	Target	Attacker	Approach	Purpose
Traditional Attacks	Unspecified, mostly individual systems	Mostly single person	Single-run, "smash and grab", short period	Financial benefits, demonstrating abilities
APT Attacks	Targeting governmental and commercial organizations and institutions	Group has a high organization and advanced capabilities in addition to having sufficient resources	Repeated penetration attempts, keep slow and low adapt to resist all detection, long-term	Competitive advantages, strategic benefits

APT attack process

APT attacks require that everything is carefully planned and executed. However, since the term has been drafted in 2006 by the United States Air Force (USAF), the series of steps used by the attackers are similar. Previous studies identified the number of steps treated to be 4 steps [17], 5 steps [16] and 18], 6 steps [19], 7 steps [20], and 8 steps [21]. However, all APTs have a common characteristic of passing the same stages to reach their target. Figure 1 shows the APT attack process, which can be summarized as mentioned below:

1. Intelligence gathering: infiltrate the company's network
2. Initial exploitation: install the required malware.
3. Command and control: Malware infiltrating search for other vulnerabilities and for further command and control. Malicious software identifies additional vulnerabilities to be used to continue the attack and access to important information, passwords and email addresses.
4. Privilege escalation: after achieving the goal, the hacker will clean the effect and leave some gaps to return at any time.
5. Data exfiltration: export the data to the hacker.

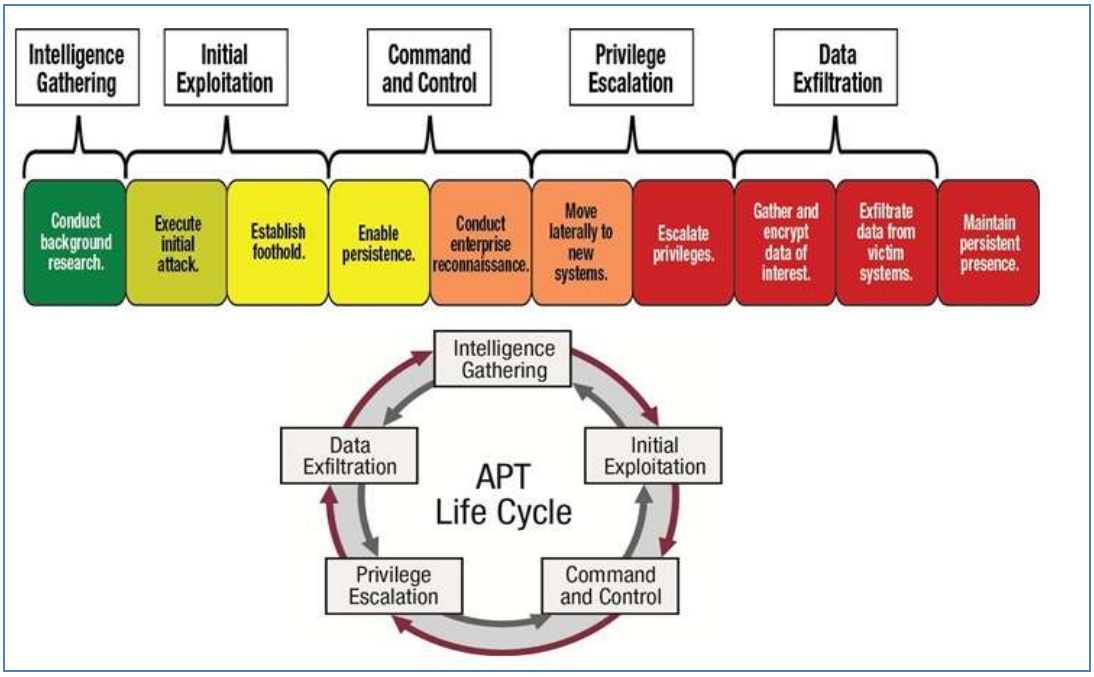

Figure 1-APT attack process. source: [22]

APT Groups and Tools

There are a huge number of APTs' names [23], but most of these names fall under the same threat groups. Each company nominates its own names on these groups. For example, APT 29 has more than 12 names, as shown in Table-2. In addition, these groups often share the same tools that are used during the hacking process. [23] shows that the number of groups used is only 174, which have a huge number of names.

From [23], it can also be noted that the sources of these groups are limited to some countries, led by China: 73, Russia: 16, North Korea: 8, Iran: 17, Israel: 2, NATO: 2, Middle East: 11, Other Actors: 20, and Unmapped Actors: 25. The tables of [23] covered more than 174 groups and operations of APTs that have appeared in multiple regions around the world. Table 3 shows that the number of tools used does not exceed 40. The table provides a valuable contribution to researchers by providing a brief summary of the malware used to implement the APT phases. The detection of APT is very difficult if the verification process takes into account the APT issue as a whole for all steps of the attack process. Therefore, we can focus on the features of these tools and sources of these groups.

Table 2- Groups and Operations of APT29 *Source: [23]*

Name	Other names	Toolset / Malware	Targets
APT29	1-Dukes, 2-Group 100, 3-Cozy Duke, 4-EuroAPT, 5-Cozy Bear, 6-CozyCar, 7-Cozer Office Monkeys , 8-TEMP.Monkeys, 9-Minidionis, 10-SeaDuke, 11-Hammer Toss, 12- Fritillary	Hammertoss, OnionDuke, CosmicDuke, MiniDuke, CozyDuke, SeaDuke, SeaDaddy implant developed in Python and compiled with py2exe, AdobeARM, ATI-Agent, MiniDionis, Grizzly Steppe, Vernaldrop, Tadpole, Spikerush, POSHSPY, PolyglotDuke, RegDuke, FatDuke	This threat actor targets government ministries and agencies in Europe, the US, Central Asia, East Africa, and the Middle East, associated with DNC attacks

We summed up more than 174 APT groups which appeared in multiple regions around the world. The paper provides a valuable contribution to researchers by providing a brief summary of malicious software that are considered as tools for APT attacks. In addition, this research proposed a new framework that can be used to repel this threat based on APT activity with network traffic through packets analysis. Previous literature suggests that most researchers focused at one or two phases for the purpose of detecting APT attacks [16].

Table 3- Malware used to implement the APT phases. *Source:* [23]

	Name 1	Other names	Family	Comment
1	Gh0st RAT	Moudoor, Piano Gh0st, Zegost,		
2	Poison Ivy	Darkmoon, PIVY,		
3	HydraQ	9002 RAT, Troj/Agent-XAL, McRAT, Naid, BKDR_MDMBOT		
4	Hikit	Matrix RAT, Gaolmay,		
5	Zxshell	Sensode,		
6	DeputyDog	Fexel,		
7	PlugX	Sogu, Destory RAT, Kaba, Korplug, TVT, Thoper	PlugX	Often uses DLL side loading
8	BACKSPACe	BARYS, Lecna		
9	Regin	WarriorPride, Prax, QUERTY		FEYES malware
10	HttpBrowser	TokenControl,		
11	NetTraveler	RedStar, TravNet, Netfile,		
12	IceFog	Fucobha,		
13	HTran	Xdoor, CTran, ONHAT (similar),		Chinese Tunneling Tool
14	Agent.BTZ	SillyFDC,		
15	Comfoo	,		RSA incident, Red October
16	DNSChanger	RSPlug,	ZLob	
17	IEXPLORE RAT	Briba, Comfoo, Sharky RAT		
18	LSB	,		
19	LStudio	Emissary, Elise,		
20	MNKit	WingD, Tran Duy Linh,		
21	Derusbi	Shyape, Photo, Mivast, Sakula (variant),	Derusbi	Winnti , Chinese Backdoor,
22	Wipbot	Epic, Tavdig,		

23	Carbon Rootkit	Snake Rootkit, Cobra,		
24	Turla	Uroburos,		
25	Winnti (Network Driver Component)	Derusbi,		Driver loaded into memory, P2P Backdoor
26	WCE	AceHash,		Password Dumper, PTH
27	Mimikatz	Powerkatz,		PTH, Password Dumper, DCSync, Golden/Silver Tickets , SkeletonKey,
28	HDRoot	HDD Rootkit,		Winnti / Axiom Group
29	OrcaRAT	LeoUnica,		Found with Comfoo malware
30	Etumbot	,		Assocaited with Numbered Panda/APT12
31	xcmd	,		Similar to Used in OPM, psexec. and Anthem breaches
32	NjRAT	,		
33	X-Agent	Fysbis,		Used by Sofacy group, Linux backdoor
34	Adwind RAT	Unrecom, Sockrat, Frutas, jFrutas, jBifrost RAT AlienSpy, jSocket, Jrat,	Adwind	
35	Jiripbot	Flacher,		Wild Neutron
36	Quasar RAT	,		
37	FallChill	Manuscrypt ,		Backdoor. Used by Lazarus Group, Bluenoroff.
38	Infy	Infy M,		
39	Mtool	MultiTool,		Cn Group Tool for Recon
40	DustySky	NeD Worm,		

Detecting APT Attack

APT detection task is not easy and needs a lot of resources. Previous literature suggests that there are three widely used approaches to detect APT attacks: change controlling, sandboxing and, network traffic analysis.

A. Change controlling

The main idea of this theory is to follow all changes that occur to sensitive and important aspects in the computer or network. If the change is illegal, you'll be alerted or acted upon. The main advantage of this approach is that it can detect new types of malware. There is no need to know the characteristics of the malware in advance. The problem is that malware can work between two of the resulting tests and change the state of the device before verifying legitimacy. The other drawback is that it does not control memory, so you should deploy additional tools for analysis. The number of features to be verified is very large (hundreds of thousands), leading to a significant slowdown in performance.

B. Sandboxing

Sandboxing is a way through which a virtual environment is given under the control of malware to run them and then analyze their observed behavior; to determine whether the files are harmful or not. Consequently, the files that are not trusted are isolated. It provides robust malware prolong, but such a process is hard to be automated, while the manual work is expensive.

C. Traffic Analysis

In order to remotely control the victim's device, attackers need to establish a command and control channel. It is responsible for sending commands and transferring data. Most malware (e.g. Gh0st, PC Share, Poison Ivy and Remote Access Tool (RAT)) often use inbound and outbound traffic. Traffic analysis is the oldest and most widely used method. In this technique, the analysts of the outbound

traffic and a sequence of features unique to the APT attack are used to detect the attack. In this case, regardless of how the machine was infected (even if the APT attack is new), the attack can be detected. However, it is too hard to analyze traffic in a large network. Detecting APT malware infections in a large network is another challenging problem [24].

To hide the intrusion, sometimes the hacker takes one of the computers as a starting point to attack the company's other internal computers (stepping stones) [25, 26]. To reduce the damage caused by APTs attack, the company needs to know APT-infected computers as quickly as possible. To solve this problem, there is a need to involve one of the methods of the stepping stone approach to detect the threat as quickly as possible.

In a published work [12], the authors noted that monitoring and analyzing network traffic leads to the detection of APT activities. They analyzed various APT campaigns such as Enfal, Taidoor, Sykipot, and IXESHE, which have been used to launch targeted attacks. These malicious programs create a connection to the command and control server using known protocols such as HTTP and are typically configured through three ports (443, 80, and 8080). Monitoring the size and timing of network traffic is another aspect to detect APT attacks.

In other investigations [27, 28], the experimental process included backdoor samples which are commonly used in APT activities. The results of these studies agreed with the studies mentioned above in that monitoring packets is an effective way to detect APT attacks. The experiment explained that the proposed method is very fast compared with other antivirus systems and IDS. Furthermore, most of the malware attacks detected by the proposed method were not detected by the previous antivirus systems or IDS.

Proposed framework

Previous studies have shown, as previously mentioned in the Introduction and Literature Review sections, that APT attacks have two weaknesses through which they can be detected. First, attackers need to establish a command and control channel. The data theft cannot be completely invisible; the theft of data needs outbound traffic. Second, all APT threats need to establish a command and control channel. Moreover, the researchers also noted that monitoring and analyzing network traffic leads to the detection of APT activities. Therefore, in our research, we relied on the traffic analysis as the best way to detect APT threats.

However, the problem that needs to be solved is the sheer amount of traffic that needs to be analysed. We solved this problem by using Destination Host Filter unit and a blacklist of host destinations based on the fact, as has been previously noted in Table 2, that the sources of these groups are limited to some countries.

The proposed framework of this paper is based on a set of logical points as described below.

1. All previous studies related to APT attacks indicated that the attacker needs to communicate with the victim several times; the first time is when the APT penetrates the system and then repeats the connection upon the transfer of information from the victim to the attacker. Communication with command and control happens often multiple times; therefore monitoring packets with huge payloads, which are sent to the same destination IP address, will help to identify any suspicious behavior.
2. When the type of the attack uses outgoing flow only, such as the APTs backdoors that make only outbound connections [29], there is no incoming flow in this scenario. We need only to monitor the outgoing repeated packets, which are headed to the same destination. Our proposed framework adopted the technique of ‘Packets Detection System‘ based on a previous work [28]. Experiments have shown that the proposed method is very fast compared to other antivirus systems and IDs. In addition, this technique can detect zero-day and encrypted malware.
3. However, it is not easy to monitor the huge number of outgoing packets. To solve this problem, we can reduce the huge number of packets that are monitored by focusing on the limited number of suspicious hosts [30]. This method is effective even for encrypted connections because the load is not checked. In addition, the method is expandable as most analyzes can be implemented in parallel. Figure 2 shows the proposed framework. Our proposed framework adopted this technique as a ‘Destination Host Filter unit’.

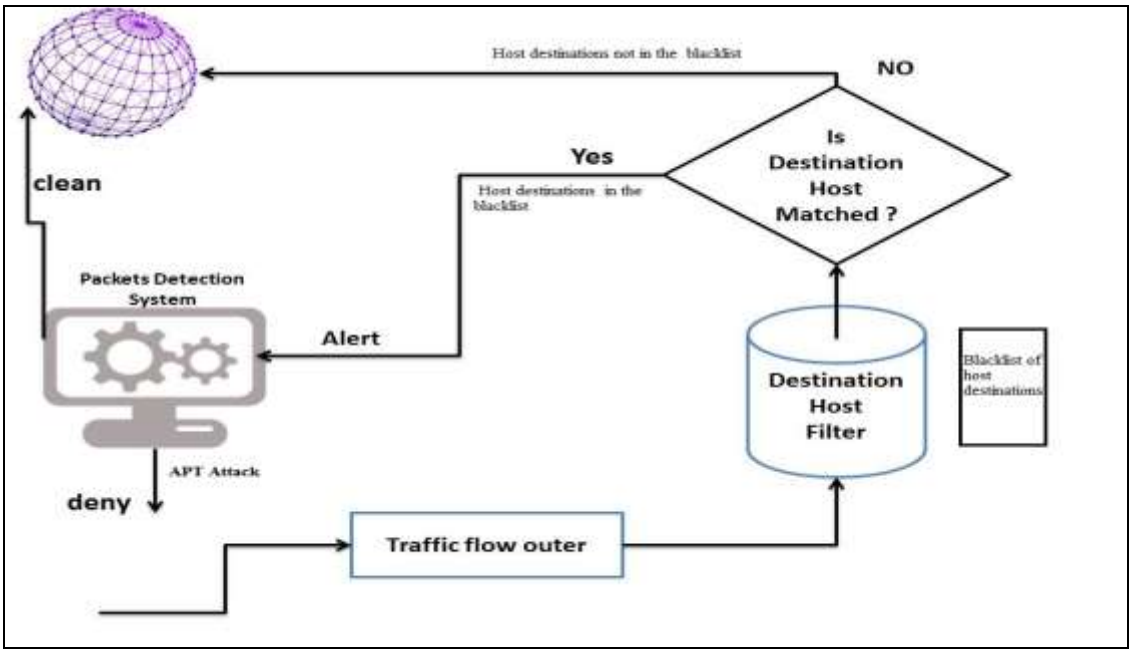

Figure 2-The proposed framework of APT Detection Based on Packets Analysis and Host Destination.

The proposed framework includes sending the flow to the Destination Host Filter unit, which matches the destination traffic host with the blacklist of stored hosts. If it is matched, the flow will convert to Packets Detection System which will issue the final decision, either to send it to the external network or to block transmission if the packets are not clean. This technique will solve the problem of monitoring the huge number of outgoing packets by focusing on a limited number of suspicious hosts.

Conclusion

The APT attack is a major problem facing information security and global networks. It is not difficult for many types of the APTs to pass the firewall of the system. APTs are more sophisticated than traditional attacks, as they use advanced evasion techniques to hide their malicious behaviour and evade all traditional detection methods. This paper describes and analyzes the APT problem by analyzing the most common techniques, tools and pathways used by attackers. Furthermore, the paper highlights the strengths and weaknesses of the existing security solutions that have been used since the threat was identified in 2006 until 2019. The paper summarized more than 174 groups and operations of APTs that have appeared in multiple regions around the world. This research also provided a valuable contribution to researchers by providing a brief summary of the malware used to implement the APT phases. In addition, this research proposed a new framework that can be used to repel this threat based on APT activity with network traffic through packets analysis.

References

1. Zimba, A., Chen, H. and Wang, Z. **2019.** Bayesian network based weighted APT attack paths modeling in cloud computing. Future Generation Computer Systems, 2019.
2. Han, W. **2019.** MalInsight: A systematic profiling based malware detection framework. Journal of Network and Computer Applications, 125: p. 236-250.
3. Ugarte-Pedrero, X., Graziano, M. and Balzarotti, D. **2019.** A Close Look at a Daily Dataset of Malware Samples. ACM Transactions on Privacy and Security (TOPS), 22(1): p. 6.
4. Jasek, R., Kolarik, M. and Vymola, T. **2013.** APT detection system using honeypots. in Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC'13), WSEAS Press.
5. Sonawane, S., Prasad, G. and Pardeshi, S. **2012.** A survey on intrusion detection techniques. World Journal of Science and Technology, 2(3).
6. Balzarotti, D. **2010.** Efficient detection of split personalities in malware. in Network and Distributed System Security Symposium (NDSS).
7. Radmand, A. **2009.** A ghost in software, [cited 2013 sep, 21]; Course]. Available from: http://cs.columbusstate.edu/cae-ia/StudentPapers/radmand.azadeh.pdf.

8. Hamed, T., Ernst, J.B. and Kremer, S.C. **2018.** A Survey and Taxonomy on Data and Pre-processing Techniques of Intrusion Detection Systems, in Computer and Network Security Essentials. 2018, Springer. p. 113-134.

9. Idika, N. and A.P. Mathur, A.P. **2007.** A survey of malware detection techniques. Purdue University, p. 48.

10. Maarof, M.A. and Osman, A.H. **2012.** Malware Detection Based on Hybrid Signature Behaviour Application Programming Interface Call Graph. American Journal of Applied Sciences, 9.

11. Slot, T. and Kargl, F. **2015.** Detection of apt malware through external and internal network traffic correlation. 2015, Master Thesis, University of Twente March.

12. Villeneuve, N. and Bennett, J. **2012.** Detecting apt activity with network traffic analysis. Trend Micro Incorporated Research Paper, p. 1-13.

13. Sharma, P.K. **2017.** DFA-AD: adistributed framework architecture for the detection of advanced persistent threats. Cluster Computing, 20(1): p. 597-609.

14. Chakkaravarthy, S.S., Vaidehi, V. and Rajesh, P. **2018.** Hybrid Analysis Technique to detect Advanced Persistent Threats. International Journal of Intelligent Information Technologies (IJIIT), 14(2): p. 59-76.

15. Haq, T., Zhai, J. and Pidathala, V.K. **2017.** Advanced persistent threat (APT) detection center. 2017, Google Patents.

16. Alshamrani, A. **2019.** A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials.

17. Lim, Y. **2013**. Review on the Cyber Attack by Advanced Persistent Threat. The Korean Association for Terrorism Studies, 2013. 6(2): p. 158-178.

18. Tankard, C. **2011**. Advanced persistent threats and how to monitor and deter them. Network security, 2011. 2011(8): p. 16-19.

19. Chen, P., Desmet, L. and Huygens, C. **2014**. A study on advanced persistent threats. in IFIP International Conference on Communications and Multimedia Security, Springer.

20. McWhorter, D. **2013**. Mandiant Exposes APT1—One of China's Cyber Espionage Units & Releases 3,000 Indicators. Mandiant, February, 18.

21. De Vries, J. **2012**. Towards a roadmap for development of intelligent data analysis based cyber attack detection systems.

22. Burazer, R. **2015**. CYBERSECURITY: ISSUES AND ISACA'S RESPONSE, 6/1/2019]; Available from: https://csa-cee-summit.eu/archive/wp-content/uploads/2015/03/Renato-Burazer.pdf.

23. Stirparo, P. **2019**. APT Groups and Operations, 02-07-2019]; Available from: https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml?cv=1.

24. Zhao, G. **2015**. Detecting APT malware infections based on malicious DNS and traffic analysis. IEEE access, 3: p. 1132-1142.

25. Alperovitch, D. **2011**. Revealed: operation shady RAT. Vol. 3. 2011: McAfee.

26. Liu, S.T., Y.M. Chen, Y.M. and H.C. **2012**. Hung. N-victims: An approach to determine n-victims for apt investigations. in International Workshop on Information Security Applications. Springer.

27. Alminshid, K. and M.N. Omar, M.N. **2013**. Detecting backdoor using stepping stone detection approach. in Second International Conference on Informatics & Applications (ICIA). 2013. IEEE.

28. Al-Minshid, K.A.A. **2014**. Backdoor attack detection based on stepping stone detection approach, Universiti Utara Malaysia.

29. Welch, V. **2012**. Security at the Cyber Border: Exploring Cybersecurity for International Research Network Connections.

30. Marchetti, M. **2016**. Analysis of high volumes of network traffic for advanced persistent threat detection. Computer Networks, 109: p. 127-141.